



## ***Intelligent Wireless Router***

### ***User Manual***

*Version: V1.0*

*Date: 2013.02.01*

Copyright :

Copyright © 2013 Shenzhen Yichen Technology Development Co., Ltd.

All rights reserved.

JCG is a registered trademark of Shenzhen Yichen Technology Development Co., Ltd.

Without the express written permission from Shenzhen Yichen Technology Development Co., Ltd., no organization or individual is allowed to imitate, duplicate, copy, translate or use for other purposes. All other trademarks or registered trademarks in this document are owned by their holders and protected by the relevant laws.

The product specifications and information mentioned in this manual are for reference only, and no further notice will be provided for possible content update. For more detailed product information, please visit our official website: <http://www.jcgcom.com>.

## *Chapter I Introduction*

Thank you for purchasing JCG 11N series WLAN router, which integrates the router, switch, wireless access point with the firewall and adopts the most advanced MIMO (multiple input multiple output) technology to increase the wireless transmission rate over 3 times of the initial 802.11g standard. It supports 64/128-bit WEP encryption and the advanced encryption and security features like WPA and WPA2. With the WPS encryption function, you can easily set up the secure wireless network environment. And with the provided setup guide, you can easily set up the router, remotely access and manage the router anytime anywhere via the Internet. JCG 11N series WLAN router is a series of cost-effective products specially designed for small-size enterprises, families and student's dormitory to meet their needs for wireless Internet access. It's the best choice for you to enjoy the wireless Internet access and the fun from wireless connectivity.

JCG 11N series WLAN router is simple to set up, which can be installed and set up using the operation manual without professional assistance. Before you are ready to install and use this product, please read the manual carefully for better understanding and use of the full functionalities of this product.

### **1.1 Purpose and Definitions**

This manual is used to help you familiarize with the JCG 11N series WLAN router and use it properly. To avoid ambiguity, we define the terms used in this manual as follows:

**Router:** refers to JCG 11N series WLAN router, unless otherwise specified.

**Modem:** network service access device. It can be xDSL, Cable Modem, GPON or EPON, etc.

**Computer/ host:** refers to desktop computer, laptop or all the network Client in a broader sense.

**NIC:** refers to the wired or wireless network interface card (NIC) for network connectivity.

**ISP:** Internet service provider, refers to the company or organization providing Internet services.

**AP:** wireless network access point, it may refer to the wireless router providing wireless network access services.



#### **7. RST/WPS button**

When the router is working, press this button for 1 second to set encryption; press this button for more than 5 seconds to restore to factory settings.

#### **8. WLAN (wireless) button**

Switch on/off the wireless network. Press this button for one second to switch on/off the 2.4G wireless network; press this button for more than 5 seconds to switch on/off the 5G wireless network.

#### **9. QoS button**

Shortly press on this button to limit the host's maximum traffic. When the QoS is in IP address limited traffic mode, limit the host to use the 1/10 of the maximum network bandwidth; when the QoS is in priority mode, limit the host to the lowest priority; when the IP connection limit is enabled, the maximum connection sessions of this host is limited to 10; shortly press this button once to switch the current limited host; press this button for more than 5 seconds to lease the bandwidth limitation on the host.

**STA:** wireless client/station, refers to wireless client devices, such as laptop, mobile phone and tablet PC etc.

**Client:** wired or wireless client, including but not limited to computer, laptop, mobile phone and tablet PC etc.

## *Chapter II Hardware Installation*



### **10. Power regulation button**

Wireless radio power regulation (\*1.\*5.\*10)

### **11. Power jack (DC IN)**

Connect to power adapter

### **12. WAN (Internet) port**

WAN port

### **13 LAN 1-4 network interface**

LAN port

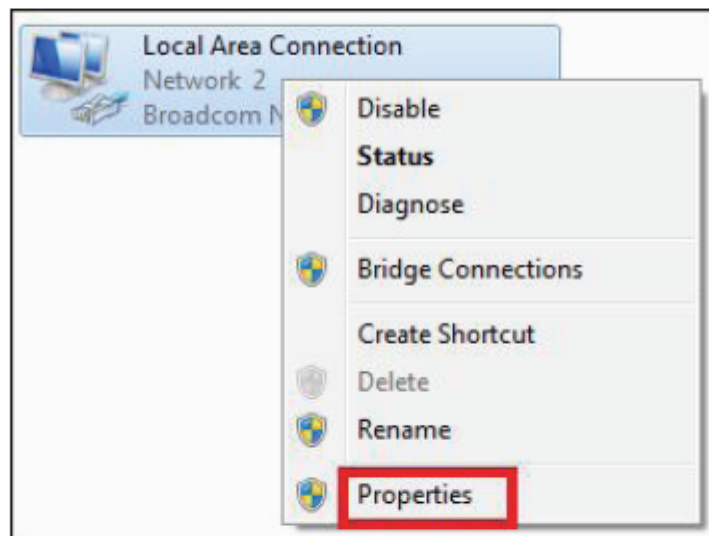
### **14. USB 2.0**

Connect to USB device, such as USB hard disk, USB thumb driver or USB printer

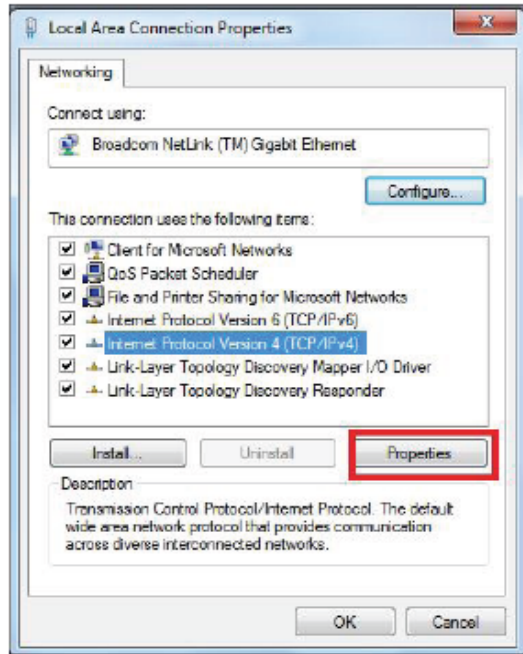
### 3.1 Set up Network Correctly (take Windows 7 as an example)

This step can be skipped if no special setup was done on your computer.

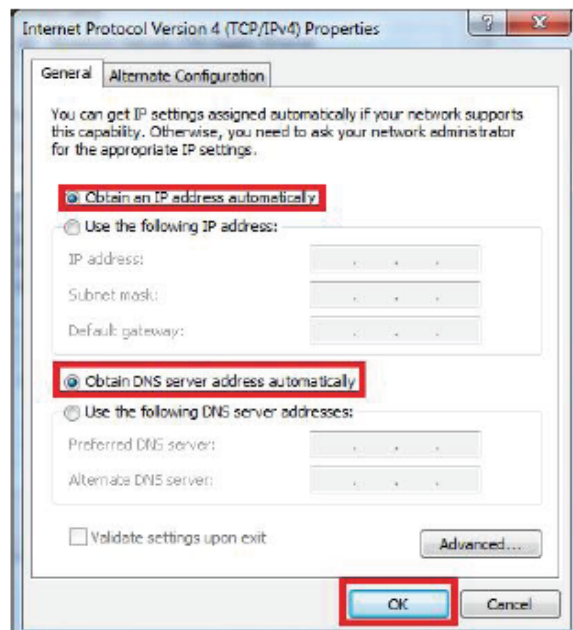
1) Click: " Start->Control Panel->Network and Internet->Network and Sharing Center->Change adapter settings->Local Area Connection" and select the connected network card. Then right click "Local Area Connection" to select Properties



2) Select **Internet Protocol Version 4(TCP/IPv4)** and click **Properties**



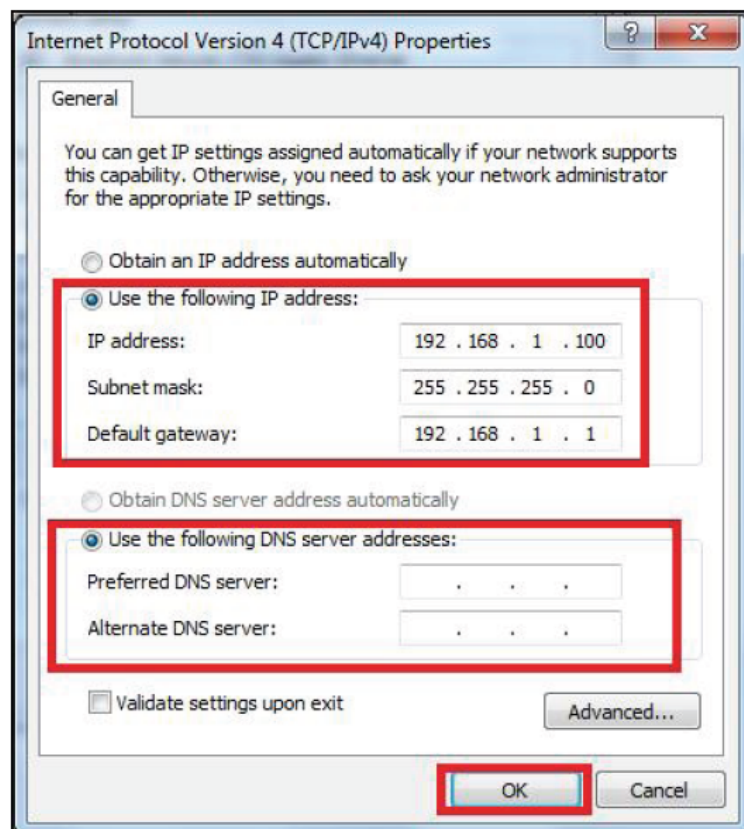
3) Select Obtain an IP address automatically, Obtain DNS Server address automatically and click OK. Return back to the previous interface and click OK. The system will automatically obtain the IP address and DNS.



We recommend setting up your network environment via automatically obtaining the IP address. If fixed IP address is required for network connection, select Use the following IP address and input the corresponding IP address, subnet mask and default gateway. Also, you can enter the corresponding DNS server on Preferred DNS server and Alternate DNS server as needed. Please contact the network service provider or our customer service for details.

**Note:**

The default IP address is in the range of 192.168.1.X ( $2 \leq X \leq 254$ ), the subnet mask is 255.255.255.0 and the default gateway is 192.168.1.1



5) Use Ping to check whether the computer and the router are connected.

Click Start and enter "cmd" in the subsequent search box and then press Enter to enter the interface as shown below.



**Note:**

If you cannot access the router setup pages, please refer to FAQ for trouble shootings.

4. After logging in successfully, click Setup Wizard4. After logging in successfully, click Setup Wizard

**Setup Wizard**

In setup wizard, you can setup the basic settings that is required for Internet surfing.

You are not required to be a network professional to use the router, setup wizard will guide you setup by setup to complete the network setup and start surfing the internet quickly.

Click 'Next' to continue the setup wizard.

Click 'Cancel' to quit the setup wizard.

Cancel

Next

**5.LAN settings**

Set the LAN IP address.

**LAN Settings**

Setup the LAN IP address for the router.

IP Address:

192.168.1.1

Netmask:

255.255.255.0

Cancel

Back

Next

**6.Wireless settings**

Wireless settings allow you to perform the basic settings on the wireless network, such as SSID and wireless channel, etc. After the settings, click Next.

If your router supports dual-band wireless network , such as JHR-N936R, the 2.4G and 5G wireless network settings will appear separately, but setting parameters are basically the same as those of 2.4G wireless network settings.



### Wireless Settings (2.4G)

In this page, you can set SSID, network mode and channel etc. for the wireless network.

Wireless Network:	<input type="radio"/> Off <input checked="" type="radio"/> On
Network Mode:	802.11 B/G/N Mixed
Network Name (SSID):	JCG-030404-2.4G
Hidden SSID:	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Channel:	6
Security Mode:	WPA2 Personal
WPA Algorithm:	<input type="radio"/> TKIP <input checked="" type="radio"/> AES <input type="radio"/> TKIPAES
Pass Phrase:	1234567890

7. Click Next to set the WAN parameters. Here you can also set the connection types. The router supports three common connection types: fixed IP, obtaining IP automatically and PPPoE dial-up.

If obtaining IP automatically is selected, the IP address does not need to set and the router will obtain the network parameter automatically from the above node.

### WAN Settings

Several WAN connection types are provided in this router, select proper connection type for your network. Consult your ISP or network administrator if you are not sure which connection type to use.

Connection Type: DHCP (Auto Config) Auto Detect

<b>Auto Detect:</b>	Detect your WAN connection type automatically.
<b>Static (Fixed IP):</b>	You need to setup the IP address, subnet mask, gateway and dns information provided by ISP or network administrator.
<b>DHCP (Auto Config):</b>	DHCP server will assign the IP address and other network parameters properly, and the router will be connected automatically.
<b>PPPoE (ADSL):</b>	You can connect the router to ADSL modem, and router will use the username and password to connect internet.

Cancel Back Next

If PPPoE connection type is selected, the following page will appear, input the username and the user password provided by the service provider.

## WAN Settings

Several WAN connection types are provided in this router, select proper connection type for your network. Consult your ISP network administrator if you are not sure which connection type to use.

Connection Type:	<input type="text" value="PPPoE (ADSL)"/>	<input type="button" value="Auto Detect"/>
User Name:	<input type="text" value="pppoe_user"/>	
Password:	<input type="password" value="....."/>	<input type="button" value="Show"/>
Confirmed Password:	<input type="password" value="....."/>	

<b>Auto Detect:</b>	Detect your WAN connection type automatically.
<b>Static (Fixed IP):</b>	You need to setup the IP address, subnet mask, gateway and dns information provided by ISP or network administrator.
<b>DHCP (Auto Config):</b>	DHCP server will assign the IP address and other network parameters properly, and the router will be connected automatically.
<b>PPPoE (ADSL):</b>	You can connect the router to ADSL modem, and router will use the username and password to connect internet.

<input type="button" value="Cancel"/>	<input type="button" value="Back"/>	<input type="button" value="Next"/>
---------------------------------------	-------------------------------------	-------------------------------------

If Static(Fixed IP) is selected, the following page will appear, input the fixed IP address, net mask, default gateway and DNS server, etc. provided by the service provider.

## WAN Settings

Several WAN connection types are provided in this router, select proper connection type for your network. Consult your ISP network administrator if you are not sure which connection type to use.

Connection Type:	<input type="text" value="Static (Fixed IP)"/>	<input type="button" value="Auto Detect"/>
IP Address:	<input type="text" value="0.0.0.0"/>	
Netmask:	<input type="text" value="0.0.0.0"/>	
Gateway:	<input type="text" value="0.0.0.0"/>	
Primary DNS:	<input type="text" value="0.0.0.0"/>	
Secondary DNS:	<input type="text" value="0.0.0.0"/>	

<b>Auto Detect:</b>	Detect your WAN connection type automatically.
<b>Static (Fixed IP):</b>	You need to setup the IP address, subnet mask, gateway and dns information provided by ISP or network administrator.
<b>DHCP (Auto Config):</b>	DHCP server will assign the IP address and other network parameters properly, and the router will be connected automatically.
<b>PPPoE (ADSL):</b>	You can connect the router to ADSL modem, and router will use the username and password to connect internet.

If you do not know which connection type to select, click Auto Detect and the router will detect the WAN connection type automatically to facilitate the settings of router.

Click Next a few times until clicking Save/Apply to restart the router. (DO NOT turn off the power during the restart process).

## 3.3 Detailed Settings

### 3.3.1 Network Settings

#### 1. Quick settings:

You can set up the network connections and wireless network parameters in just one step, and enjoy the fun of Internet surfing.

#### 2. LAN settings:

LAN settings allow you to set the IP address range, netmask allocated by the DHCP server and the router IP address based on actual needs. If you do not know how to set, please contact the network administrator or keep the default settings.

**LAN Settings**

Host Name:	JCG-030403
IP Address:	192.168.1.1
Netmask:	255.255.255.0
MAC Address:	00:01:02:03:04:03

**DHCP Settings**

DHCP Server:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Start IP Address:	192.168.1.100
End IP Address:	192.168.1.199
Default Gateway:	192.168.1.1
Block none DHCP IP address:	<input type="checkbox"/>
DNS Server:	<input type="radio"/> Static <input checked="" type="radio"/> Dynamic
Lease Time:	1440 mins
Static IP Binding:	Static IP

IP address—IP address of the router

Netmask- it controls the host number that can be accommodated by the network. Keep the default settings if there are no special needs.

Start IP address —the start IP address offered by the DHCP.

End IP address—the end IP address offered by the DHCP.

Static specify [MAC: IP]—you can bind a fixed IP address to the device with the specified MAC address.

**Note:**

a. If the IP of LAN port is modified, please use the new address to access the router.

b. If the new IP address and the original IP address are not in the same network segment, the firewall rules, NAT rules, static DHCP, ARP binding and QoS rules may require reset. Therefore, it's better to set the LAN IP address before doing other settings.

c. If the DHCP server is disabled, you may need to manually set the IP address of the computer before accessing the router setting pages.

**3. WAN settings:**

WAN settings allow you to select the suitable WAN connection type based on the network environment, and set the necessary parameters specific to different connection types. If you don't know the connection type and the parameters, please contact the network administrator or ISP.

**WAN Settings**

Connection Type:	<input type="text" value="DHCP (Auto Config)"/>	
Host Name:	<input type="text" value="JCG-030402"/>	(Optional)
Max. Transmission Unit (MTU):	<input type="text" value="1500"/>	(Default: 1500)
Static DNS:	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	

Static (fixed IP)—it allows you to set the fixed IP address allocated by the network administrator or ISP. In this type, you are also required to set the Netmask, default gateway and DNS correctly.

DHCP (automatically obtain IP)—it allows you to automatically obtain the IP address, Netmask, DNS and other relevant information through the remote DHCP server and connect automatically.

PPPoE dialing—it allows you to connect the router to the ADSL modem or to the device requiring PPP dialing connection, and then access the Internet through PPPoE dialing.

PPTP/L2TP VPN\* -- if the network type provided by the ISP is PPTP/L2TP, ISP will provide the account and password. For the unclear parts during the detailed settings,

please contact the ISP provider.

MAC address Clone—it allows you to regard the MAC address of LAN card or the specified MAC address as that of WAN. If your MAC address has been bound, MAC address Clone may help you.

\* Only some routers in some countries or regions support it.

#### 4. Routing settings:

Static router allows you to specify the forward routing for the special host or network. Then any access to this host or network will not be forwarded through the default routing. This situation applies to the LAN port with another router R2 connecting to this router R1.

For example: setting LAN network static routing: as shown in the figure, all of the internal R2 LAN hosts can access the host internal the R1 LAN. But if the hosts of the R1 LAN want to access that of R2 LAN, the static routing of R1 is required to be set as follows:

Dest. IP address: 192.168.0.1 (LAN address of R2)

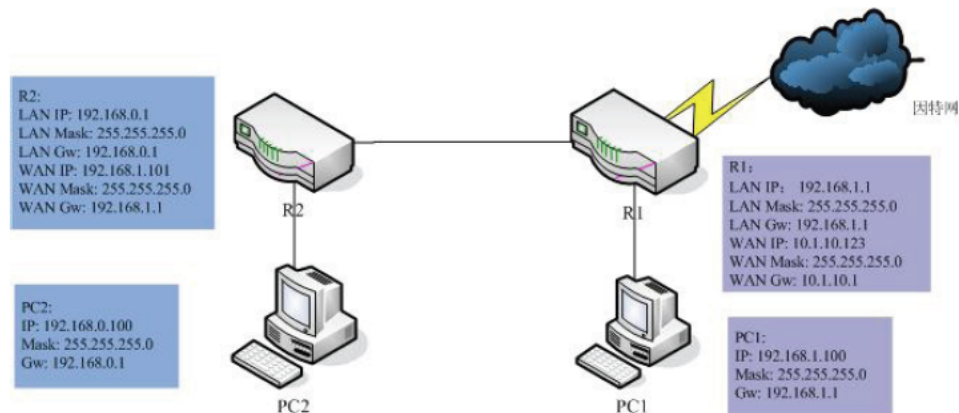
Routing range: network

Netmask: 255.255.255.0 (netmask of R2)

Gateway IP address: 192.168.1.1 (WAN IP address of R2)

Network interface: LAN

After the setting, R1 internal host and R2 internal host should be able to communicate with each other



**Static Routing Settings**

Dest. IP Address:	<input type="text"/>
Routing Type:	<input checked="" type="radio"/> Host <input type="radio"/> Network
Gateway:	<input type="text"/>
Interface:	LAN <input type="button" value="v"/>
Comment:	<input type="text"/>

**Dest. IP address**—IP address of destination host or network, such as the IP address of the device connecting to the router at a lower level or its net address.

**Gateway IP address**—IP address of the gateway, such as the IP address of the lower-level router connecting to this router.

## 5. Connection parameters

Set the network connection parameters of the routers for better connection performance. 0 means to use the system default value.

**Connection parameter Settings**

Max Connections:	<input type="text" value="8192"/>	(512~99999, Default: 8192)
Generic Timeout:	<input type="text" value="600"/>	Seconds (Default: 600)
ICMP Timeout:	<input type="text" value="30"/>	Seconds (Default: 30)
TCP CLOSE Timeout:	<input type="text" value="10"/>	Seconds (Default: 10)
TCP CLOSE WAIT Timeout:	<input type="text" value="60"/>	Seconds (Default: 60)
TCP ESTABLISHED Timeout:	<input type="text" value="180"/>	Seconds (Default: 180)
TCP FIN WAIT Timeout:	<input type="text" value="120"/>	Seconds (Default: 120)
TCP LAST ACK Timeout:	<input type="text" value="30"/>	Seconds (Default: 30)
TCP SYN RECV Timeout:	<input type="text" value="60"/>	Seconds (Default: 60)
TCP SYN SENT Timeout:	<input type="text" value="20"/>	Seconds (Default: 20)
TCP TIME WAIT Timeout:	<input type="text" value="120"/>	Seconds (Default: 120)
UDP Timeout:	<input type="text" value="180"/>	Seconds (Default: 180)
UDP STREAM Timeout:	<input type="text" value="180"/>	Seconds (Default: 180)



Max. connections-- modifying the connections appropriately allows the router to open more connections at the same time. But the max connections may be limited by the router memory and too many connections will result in breakdown of the router due to insufficient memory! Please modify this parameter carefully.

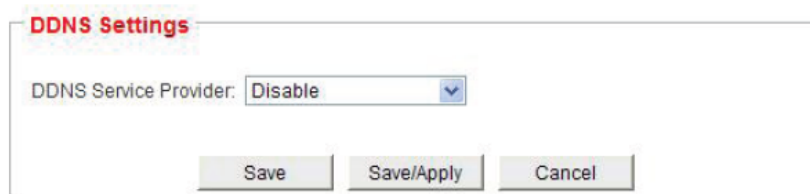
Timeout—modifying the connection timeout appropriately can reduce the connection time of the occupied resources for better network performance. But the too long or too short timeout may cause certain applications fail to work! Please modify such parameters carefully.

**Note:**

A good understanding of network technology is required before modifying these network connection parameters. Keep the default values if you are unsure of the roles of these parameters!

**6. DDNS settings\*:**

DDNS(Dynamic Domain Name Service) allows you to access the router with domain name through WAN. A legitimate account of DDNS service provider is required to be registered before using this function.



DDNS Settings

DDNS Service Provider: Disable

Save Save/Apply Cancel

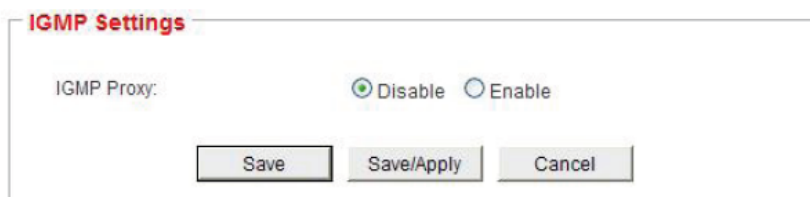
**Note:**

For using DDNS function, please allow the remote management function in Firewall Settings->System Security.

\* The DDNS service providers in some countries or regions may differ

**7.IGMP Settings\*:**

IGMP Proxy monitors the IGMP packets between hosts and the router and setup multicasting tables for the host to work properly. It's useful for IPTV STB.



IGMP Settings

IGMP Proxy: ☒ Disable ☐ Enable

Save Save/Apply Cancel



\* This function may have limited help on IPTV or not be supported by IPTV service providers depending on different IPTV service providers. Please contact IPTV service providers for detail.

### 8. Guest Access

Guest access can be used to provide Internet surfing service for guest hosts. The hosts connect to guest network are not able to communicate with the hosts in common LAN networks.

**Guest Access Settings**

Guest IP Address:

192.168.01 (0-99)

JCG-030404-5G:

☒ Disable ☐ Enable

JCG-030404-2.4G:

☒ Disable ☐ Enable

Save

Save/Reboot

Cancel

### 3.3.2 Wireless Settings

If the purchased routers support dual-band wireless network, there will be independent menus to set the 2.4G and 5G wireless network parameters of the router separately. The setting methods are basically the same.

#### 1. Basic settings:

Here you can set the basic parameters of the wireless network, such as network name (SSID), security isolation, wireless channel and network mode, etc. The router can support multiple SSID to work together.

**Basic Settings**

Driver Version:	2.5.0.11
MAC Address(BSSID):	00:01:02:03:04:04
Wireless Network:	<input type="radio"/> Off <input checked="" type="radio"/> On
Network Mode:	802.11 B/G/N Mixed ▼
Network Name(SSID):	JCG-030404-2.4G
	Hidden <input type="checkbox"/> Isolated <input type="checkbox"/>
	Station Num. 0 (0~255)
Network Name 2:	
	Hidden <input type="checkbox"/> Isolated <input type="checkbox"/>
	Station Num. 0 (0~255)
Network Name 3:	
	Hidden <input type="checkbox"/> Isolated <input type="checkbox"/>
	Station Num. 0 (0~255)
Network Name 4:	
	Hidden <input type="checkbox"/> Isolated <input type="checkbox"/>
	Station Num. 0 (0~255)
AP Isolation:	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Channel:	6 ▼

SSID -- Service Set Identifier. It's the network name shared by all devices in the wireless network, also the identification of wireless access point.

Hidden SSID—it hides your AP which then can't be found out by others. Please note that in this case, you are required to set the correct SSID for your wireless device.

SSID isolated—if it's enabled, the clients connecting to the same SSID will be isolated and then can't communicate with each other directly. SSID isolation can effectively improve the security of your wireless network.

AP isolated—if it's enabled, the clients connecting to the same SSID will be isolated and then can't communicate with each other directly. AP isolation can effectively improve the security of your wireless network.

Wireless channel\*-- a suitable channel can be set for AP. If the signal is unstable, try to change the channel.

\* The allowable wireless channel range may differ depending on the selected countries or regions. Please comply with the laws of your country or region applicable to the device.

## 2. Advanced Settings

Advanced settings could be used to set advanced parameters of wireless network.

**Advanced Settings**

802.11 B/G Protection:	Auto.	
Beacon Interval:	100	ms (20-999, Default: 100)
DTIM (DTIM):	1	(1-255, Default: 1)
Fragment Threshold:	2346	(256-2346, Default: 2346)
RTS Threshold:	2347	(1-2347, Default: 2347)
TX Power:	100	% (1-100, Default: 100)
Short Preamble:	<input type="radio"/> Disable	<input checked="" type="radio"/> Enable
Short Slot:	<input type="radio"/> Disable	<input checked="" type="radio"/> Enable
Tx Burst:	<input type="radio"/> Disable	<input checked="" type="radio"/> Enable
Packet Aggregate:	<input type="radio"/> Disable	<input checked="" type="radio"/> Enable
Country/Region:	United States	

**BG protected mode** -- BG protected mode is a kind of self-adjusting mechanism which could maintain the bandwidth to balance the transmission rate among clients.

**Beacon interval** -- Beacon is a small data package for AP to synchronize wireless network. Beacon interval is the time interval of AP sending two beacons.

**DTIM** -- Delivery Traffic Indication Map. DTIM is used for informing the client that multicast or broadcast data caching on AP would be immediately transmitted after beacon frame. AP will regularly detect caching data according to DTIM value. For example, 1 indicates caching data needs detecting after each beacon.

**Fragment threshold** -- Fragment threshold value determines the size of the data package for fragmentation (how many times a data block will be fragmented). This value could be set smaller in an environment with unstable traffic or serious interference. It could help to improve network performance.

**RTS threshold** -- RTS (Request to Send) threshold value determines the size of the data package for AP to send a RTS clean-up channel before sending data. Lower RTS threshold value works better if there are many, a few or even one connected clients or clients are quite far away.

**TX power** -- Transmitted power allows to adjust the effective range and network coverage of RF. For example, 80 could be input to adjust if the transmitted power of RF needs adjusting to be 80% of the rated power.

**Short Preamble** -- It is the performance parameter of 802.11 BG mode of which some early 802.11b clients may not support though. This parameter could be used if this kind of client does not exist in the network.

Short Slot -- It is used for shortening the communication time between AP and clients.

Tx Burst -- AP attempts to send multiple packets when receiving ACK response from the client. It allows AP to maintain a larger throughput in the same time and network environment.

Package Aggregate -- It could reduce network bandwidth seized by control to assemble multiple small data packages into a large data package for transmission; however, it may reduce network performance in an environment with unstable traffic or serious interference.

WMM -- It is used for improving the data transmission performance of wireless network for multimedia contents. WMM function only works after activation.

A PSD -- Automatic power-saving transmission mode. It allows to save electric energy if there is no data transmission. It may reduce wireless performance after activation.

### 3. Security Settings

The security mode and encryption type etc. of wireless network could be set here to prevent clients from accessing your wireless network without permission.

**Network Name**  
Select Network Name (SSID): JCG-030404-2.4G ▼

**"JCG-030404-2.4G"**  
Security Mode: WPA2 Personal ▼

**WPA Settings**  
WPA Algorithm: ☐ TKIP ☒ AES ☐ TKIP/AES  
Pass Phrase: 1234567890  
Key Renewal Interval: 3600 sec (0 ~ 4194303)

**Note:**

When key length is 64, please enter 10 hexadecimal characters or 5 ASCII characters;  
when key length is 128, please enter 26 hexadecimal characters or 13 ASCII characters.

This router is provided with wireless network password in factory default. Please refer to the label on the back of the case for details.

#### 4. Access Control

**Access Control**

Select Network Name (SSID): JCG-030404-2.4G

Access Policy: Disable

Station MAC Addresses (Format: XX:XX:XX:XX:XX:XX)

MAC01:		MAC02:	
MAC03:		MAC04:	
MAC05:		MAC06:	

Access Control -- Set access control policy for stations.

Allow -- Only allow stations in the list accessing wireless network.

Reject -- Reject stations in the list accessing wireless network.

#### Note:

If you are using wireless network to connect and set the router, please fill in MAC address of WIFI of current computer in the access list when access policy is revised as Allow, otherwise the wireless router could not be connected.

#### 5. WDS Settings

Wireless distribution system (WDS) allows to conveniently extend wireless network. All AP needs to work in the same channel if WDS function is to be used. If needed, please add MAC address corresponding to AP to the list. Please make sure that the added base points support WDS function.

**WDS Settings**

WDS Mode: Disable

Save Save/Apply Cancel

Lazy mode -- In this mode, AP could be used as main access point so that other WDS base points could extend wireless network range.

Bridge mode -- AP is working in bridging mode. MAC address of WDS base points of intercommunication needs to be added to the list.

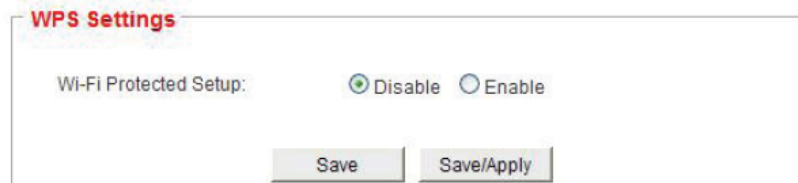
#### Note

In this mode, it receives data from a WDS base point and transmits them to other WDS base points. Therefore, it does not accept connection requests from clients.

Repeater mode -- AP is working as WDS base point. MAC address of WDS base points of intercommunication needs to be added to the list. Please disable DHCP server in this mode.

## 6. WPS Settings

Wi-Fi Protection Setup(WPS) is used for simplifying security settings and network management of Wi-Fi wireless. It supports two modes currently: PIN mode and PBC mode. The proper mode could be selected according to support from the client. Security settings could be automatically conducted through WPS, AP and the client by simply pressing the button or inputting PIN. In some clients or routers, WPS is also called WSC (Wi-Fi Simple Configuration) or QSS (Quick Security Setup).

The image shows a web-based configuration window titled "WPS Settings". Inside the window, there is a label "Wi-Fi Protected Setup:" followed by two radio buttons: "Disable" (which is selected, indicated by a green dot) and "Enable". At the bottom of the window, there are two buttons: "Save" and "Save/Apply".

WPS Settings

Wi-Fi Protected Setup: ☒ Disable ☐ Enable

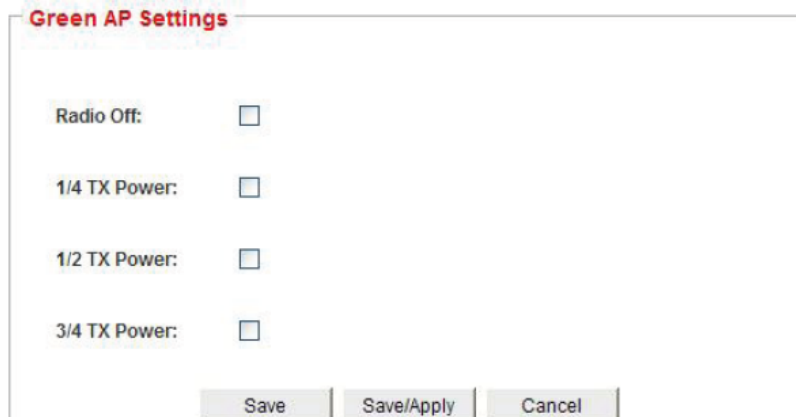
Save Save/Apply

PIN: Personal Identification Number, select PIN mode, input the PIN number of the station, and click 'Apply' to start the WPS process.

PBC: Push Button Communication, select PBC mode, and click the 'Apply' or WPS Button to start the WPS process.

## 7. Green AP Settings\*

Green AP can be used to control the wireless radio. You can turn off or reduce the Tx power for different time periods.

The image shows a web-based configuration window titled "Green AP Settings". Inside the window, there are four settings, each with a checkbox: "Radio Off:", "1/4 TX Power:", "1/2 TX Power:", and "3/4 TX Power:". All checkboxes are currently unchecked. At the bottom of the window, there are three buttons: "Save", "Save/Apply", and "Cancel".

Green AP Settings

Radio Off: ☐

1/4 TX Power: ☐

1/2 TX Power: ☐

3/4 TX Power: ☐

Save Save/Apply Cancel

Radio Off: Turn off the wireless radio, to reduce the power cost.

Tx Power Adjust: Adjust the Tx power of wireless radio.

\* Only some models support green wireless function



**Note:**

Do NOT set same time period for different actions, otherwise, the green AP function may not work properly! The timer may be invalid if the router is powered off or rebooted. Please resynchronize the timer if the router is failed to synchronize with the NTP server, otherwise, the green AP may not work properly.

**8. IDS\***

IDS Settings: Set intrusion threshold to prevent flood attacking from stations.

**IDS Settings**

Intrusion Detection System (IDS):

☐ Disable ☒ Enable

Authentication Flood Threshold:

(0~65535, Default: 0)

Association Request Flood Threshold:

(0~65535, Default: 0)

ReassocRequest Flood Threshold:

(0~65535, Default: 0)

Probe Request Flood Threshold:

(0~65535, Default: 0)

Disassociation Flood Threshold:

(0~65535, Default: 0)

Deauthentication Flood Threshold:

(0~65535, Default: 0)

EAP Request Flood Threshold:

(0~65535, Default: 0)

Threshold -- Threshold of attacking. 0 indicates no threshold.

\* Only some models support IDS

**3.3.3 NAT Settings****1. Port Forwarding/Port Mapping**

Port forwarding/port mapping allows you to provide public service of WAN in some host of LAN, such as FTP and WEB service etc. Forwarding port or port range should be designated to inform the router to forward the request received by the port from WAN to the host providing services. Sometimes, Port forwarding is also called virtual service.

**Forwarding Rule**

ID	IP Address	Protocol	Int. Port	Ext. Port	Comment	Enable
1	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text" value="80"/>	<input type="text" value="8000"/>	HTTP	<input type="checkbox"/>
2	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text" value="21"/>	<input type="text" value="21"/>	FTP	<input type="checkbox"/>
3	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text" value="23"/>	<input type="text" value="23"/>	Telnet	<input type="checkbox"/>
4	<input type="text"/>	UDP <input type="button" value="v"/>	<input type="text" value="69"/>	<input type="text" value="69"/>	TFTP	<input type="checkbox"/>
5	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text" value="22"/>	<input type="text" value="22"/>	SSH	<input type="checkbox"/>
6	<input type="text"/>	UDP <input type="button" value="v"/>	<input type="text" value="53"/>	<input type="text" value="53"/>	DNS	<input type="checkbox"/>
7	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text" value="110"/>	<input type="text" value="110"/>	POP3	<input type="checkbox"/>



Port forwarding -- Single port forwarding could set different internal and external ports for some services.

IP address -- IP address of server host is the one of local host that provides services.

Protocol -- For networking protocol used by server program, DNS server uses UDP while WEB server uses TCP etc. Both could be selected if it is not clear.

Internal port -- It is the internal network port monitored by LANS.

External port -- It is the Internet port. The router will transmit the request from the port to internal port of designated LAN host.

### Note

Forwarding ports could not be overlapped. The same external port could only be forwarded to a host.

## 2. DMZ Settings

In some cases, you may need to set DMZ host to open all its ports to Internet.



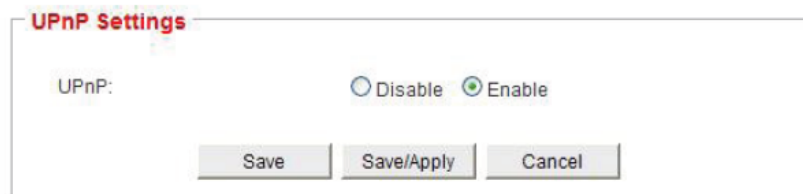
The screenshot shows the 'DMZ Settings' window. It has a title bar 'DMZ Settings'. Inside, there is a label 'Demilitarized Zone (DMZ):' followed by a dropdown menu currently set to 'Disable'. At the bottom, there are three buttons: 'Save', 'Save/Apply', and 'Cancel'.

### Note:

DMZ host will lose protection from firewall, and be exposed to the Internet.

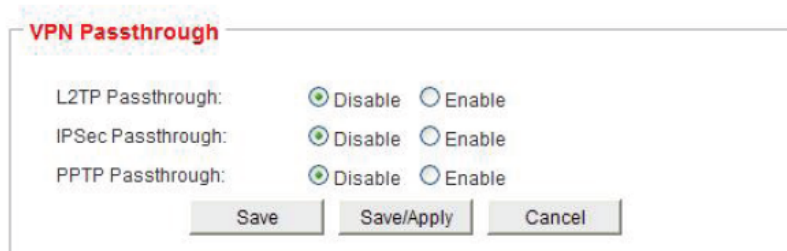
## 3.UPnP Settings

UPnP (Universal Plug and Play) is used to forward ports automatically for some applications.



The screenshot shows the 'UPnP Settings' window. It has a title bar 'UPnP Settings'. Inside, there is a label 'UPnP:' followed by two radio buttons: 'Disable' and 'Enable'. The 'Enable' radio button is selected. At the bottom, there are three buttons: 'Save', 'Save/Apply', and 'Cancel'.

## 4.Passthrough



The screenshot shows the 'VPN Passthrough' window. It has a title bar 'VPN Passthrough'. Inside, there are three labels with corresponding radio buttons: 'L2TP Passthrough:', 'IPSec Passthrough:', and 'PPTP Passthrough:'. Each label has 'Disable' and 'Enable' radio buttons, all of which are currently selected. At the bottom, there are three buttons: 'Save', 'Save/Apply', and 'Cancel'.

**FTP Passthrough**

Non-standard FTP Ports:

VPN Passthrough -- VPN passthrough allows you to set ALG (Application Layer Gateway) for L2TP, IPsec, and PPTP applications.

FTP Passthrough -- Set non-standard FTP ports to support connections to FTP services that are not using standard ports.

### 3.3.4 Firewall Settings

Objects that could be set to be filtered here are IP address, MAC address, website, domain name, application program and Internet content etc.

**Filtering** | IP Filtering | MAC Filtering | URL Filtering | Host Filtering | App. Filtering |

**Filtering Settings**

Filtering Firewall: ☒ Disable ☐ Enable

IP Filtering -- Filtering by local and remote IP address and ports.

MAC Filtering -- Filtering by the MAC address of local host.

URL Filtering -- Filtering by the key word of URL.

Host Filtering -- Filtering by the key word of host.

System security:

The router could be protected from external attack through system security settings. Remote management allows you to access and set the router through WAN; PING package of WAN allows you to inhibit PING package sniffer from WAN; SPI firewall allows to track the status of each request from WAN and prevent potential illegal attack from hackers; log on the router to set: allowed IP addresses that could log on the router to change setting. Blank list indicates no restriction. After setting login through IP address, only the IP in the list could log on the router's interface.

**System Security Settings**

Remote Management:	<input checked="" type="radio"/> Disable	<input type="radio"/> Enable
Filtering Ping form WAN:	<input checked="" type="radio"/> Disable	<input type="radio"/> Enable
Block Port Scanning:	<input checked="" type="radio"/> Disable	<input type="radio"/> Enable
Block SYN Flood:	<input checked="" type="radio"/> Disable	<input type="radio"/> Enable
SPI Firewall:	<input checked="" type="radio"/> Disable	<input type="radio"/> Enable

**IP Login Settings**

<p><b>WAN</b></p> <div> <input type="text"/> <input type="button" value="Add"/> </div> <div> <input type="text"/> <input type="button" value="Del"/> </div> <p>IP Address</p>	<p><b>LAN</b></p> <div> <input type="text"/> <input type="button" value="Add"/> <input type="button" value="Select..."/> </div> <div> <input type="text"/> <input type="button" value="Del"/> </div> <p>IP Address</p>
---	--

### 3.3.5 QOS Settings

Set network bandwidth of QoS and QoS Policy.

**Bandwidth Settings**

QoS Service:	<input type="button" value="Enable"/> ▾
QoS Policy:	<input type="radio"/> Based on Priority <input checked="" type="radio"/> Based on IP Address
Upload Bandwidth:	<input type="text" value="2M"/> <input type="button" value="bps"/>
Download Bandwidth:	<input type="text" value="8M"/> <input type="button" value="bps"/>

Bandwidth settings – Upload and download bandwidth of the router should be restricted. They are usually set to be larger than or equal to network bandwidth provided by ISP.

Based on priority -- QoS service is set on the basis of priority. Different QoS services could be provided for designated rules according to priority through reserving different upload and download bandwidth for different priorities and designating different priorities to corresponding rules. QoS rules could be set according to IP address, network and application program etc.

Based on IP address – Bandwidth control on the basis of IP address could realize redistribution and restriction on bandwidth resources through restricting the bandwidth of single IP address (or IP address range).

Classifier -- Classifiers cluster the streaming into queues to provide different QoS for hosts,

protocols, applications etc

**Classifier Add**

Classifier:

Priority:

Local IP Address:  -

DSCP:

Protocol:

Packet Length:  -  (ex: 0-128 for small packets)

Default Classifiers: We have set default QoS classifiers for some common applications and protocols, trying to use them first if you are not sure how to setup the QoS classifiers.

**Default Classifiers**

ID	Classifier	Priority	IP Address	DSCP	Protocol	Classifier Info.
1	SP_HIGH	High				Packet Length: 1 - 128
2	ICMP_HIGH	High			ICMP	
3	DNS_HIGH	High			UDP	Remote Port Range: 53
4	POPMAIL_HIGH	High			Application	App. Name: pop3
5	MAILIMAP_HIGH	High			Application	App. Name: imap
6	MAILSMTP_HIGH	High			Application	App. Name: smtp

IP Bandwidth Limit -- IP bandwidth limit is able to limit the bandwidth of per IP address (or IP address range).

**Rule Add**

Description:

Local IP Address:  -

Upload bandwidth:  -  Kb/s

Load bandwidth:  -  Kb/s

IP Connection Limit -- IP connection session limit is able to limit the connection sessions of

per IP address or IP address range.

IP Connection Limit: ☐ Disable ☒ Enable

**Rule Add**

Description:

Local IP Address:

 - 

Sessions:


Add

Cancel

### 3.3.6 USB Settings \*

#### 1.Disk management


Partitions and directories in current portable storage devices are displayed and directories could be freely added, modified and deleted.

 Kingston DataTraveler G2 ( 8015 MB )  
Storage Disk 

Remove Disk

Partition: 

/media/sda1 (C:) ▼



File System: FAT32, 4.78 GB Available, Total 7.46 GB

**Directory List**

Select	Directory
<input type="radio"/>	Manual
<input type="radio"/>	jcg
<input type="radio"/>	Media

#### 2.User management

Settings of adding, modifying and deleting are conducted for users of file sharing and FTP sharing.

**User List**

Select	User Name	Comment
--	Anonymous	Anonymous

Add

Edit

Delete

Click "Add" (for example, add a user with user name and password of jcg)

\* Only some routers with USB interfaces support this function

**User Add**

User Name:

Password:

Conform password:

comment:

The following figure is displayed after clicking OK, which indicates it is successful to add the new user:

**User List**

Select	User Name	Comment
—	Anonymous	Anonymous
<input type="radio"/>	jcg	

### 3.Samba Server

Samba server is used to share files in the network between network workstations.

**Samba Settings**

Samba Server: ☐ Disable ☒ Enable

Work Group:

NetBIOS Name:

**Sharing Directories**

User:

Partition	Directory	R/W	R	No
C:	Manual	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
C:	jcg	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
C:	Media	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

After enabling file sharing, the limit of authority on users accessing files selected by disks could be set in shared directory column, including three different limits of authority on writing, reading and no access.

#### Note:

The setting only takes effect after clicking "save/apply"! For how to access file sharing, please refer to FAQ.

#### 4. FTP Server

Set configure of FTP server parameters and access capacities.

**FTP Settings**

FTP Server:

☐ Disable ☒ Enable

Server Name:

JCG-030403

Anonymous Login:

☒ Disable ☐ Enable

FTP Port:

21

Max. Sessions:

10

**Capacity Setting**

Username

jcg

Partition	Directory	R/W	R	No
C:	Manual	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
C:	jcg	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
C:	Media	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Relevant data could be uploaded and downloaded through FTP server for corresponding users in LAN to use.

FTP port: It is suggested to set to default 21 for FTP server port.

#### Note:

The anonymous can access path of public in first part only! Please put the files which allowed in the folder of public.

For how to access FTP sharing, please refer to FAQ.

#### 5. iTunes sharing \*

Through simple setting, iTunes server in LAN could share media files in USB disk

Media files in USB disk could be shared in LAN through using iTunes server. Supported file formats are MOV, MP4, MP3, M4V, M4A and M4P.

**iTunes Server Settings**

iTunes Server:

☐ Disable ☒ Enable

Server Name:

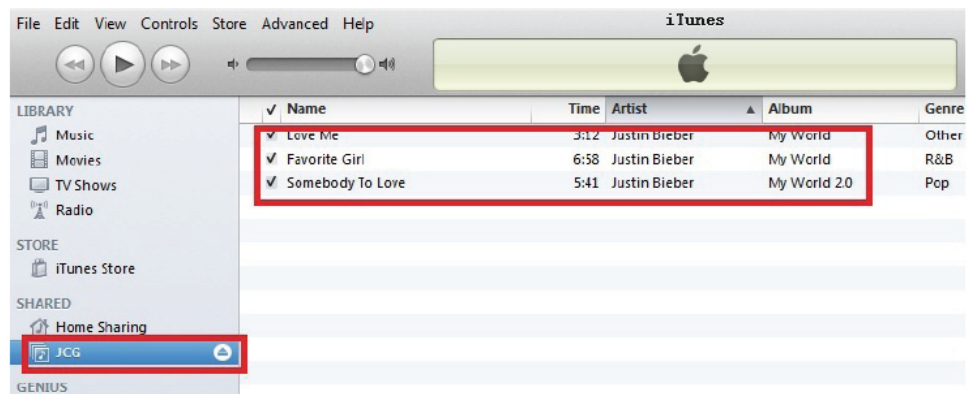
JCG

**Media Library Selection**

Select	Partition	Directory
<input type="radio"/>	C:	public
<input type="radio"/>	C:	Manual
<input type="radio"/>	C:	jcg
<input checked="" type="radio"/>	C:	Media



## Use iTunes\*\*



\* iTunes is the equipment management software of Apple Inc. iTunes sharing heavily depends on the proprietary protocol of Apple Inc. which may modify or cancel support for this protocol in any time and any circumstance.

\*\* The interface may differ with different iTunes version. iTunes sharing only supports iTunes program running on Windows system and Mac OS X system, but does not support all iOS equipments, including but not limited to iPhone, iPad and iPod etc.

## 6. Media Server

Share your media library in the USB storage disk via media server in the local network, and enjoy sharing video, photo, audio files with DLNA/UPnP supported devices.

**iTunes Server Settings**

Media Server:

☐ Disable ☒ Enable

Xbox Compatible:

☒ Disable ☐ Enable

Server Name:

**Media Library Selection**

Partition	Directory	Enable
C:	Manual	<input type="checkbox"/>
C:	jcg	<input type="checkbox"/>
C:	Media	<input type="checkbox"/>

For how to use media sharing, please refer to FAQ.

**Language Settings**

Language:

**Administrator Settings**

Account:

Password:

Confirmed Password:

**NTP Settings**

Current Time:

Time Zone:

NTP Server:

NTP Sync. Interval:  hour

**Note:**

The time information will be lost if you switch off the router and will be resynchronized when the router is reconnected.

## 2. Operation Mode

The router can work in different modes, select proper operation mode for your network topology.

**Operation Mode**

☐ Bridge (AP) All ethernet and wireless interfaces are bridged together and access internet from an ethernet port.

☒ Gateway (Router+AP) The first ethernet port serves as WAN port. Other ethernet ports and wireless interfaces are bridged together and serve as LAN ports.

☐ AP Client (Router+Client+AP) The wireless apcli interface serves as WAN port, other wireless interfaces and ethernet ports are bridged together and serve as LAN ports.

☐ AP Client Repeater (Client Repeater+AP) The wireless apcli interface serves as outgoing port, other wireless interfaces and ethernet ports are bridged together and serve as LAN ports.

Q 2: I've forgotten the user name and password of JCG wireless router, what should I do?  
If you've forgotten the user name and password of the router, you could restore the router to factory default. The router will be reset and restarted if the Reset button on the panel of the router is pressed for over 5 seconds and then released.

**Note:**

Reset button and WPS encryption key are the same one for some models. The router will be encrypted by pressing this key for 1s whereas it will be reset by pressing this button for 5s. After resetting, the default login IP of the router is 192.168.1.1 with "admin" being the default user name and password. When logging on, please make sure that IP address of the computer is within 192.168.1.X (X is any integer from 2 to 254).

Q 3: Why a laptop cannot search wireless signal?

- 1.If the laptop has a build-in WIFI, please confirm it has been enabled.
2. Check whether WIFI of the laptop is enabled. The method is as follows: right click "My Computer" on desktop and choose "Manage". Select "Services and Applications" in computer management and then check the status of "Wireless Zero Configuration" in "Services" page.  
If the status is not enabled, please right click "Wireless Zero Configuration" and enable it. If starting status is disabled, please right click to select properties, change starting status to automatic and change the status to enabled.

**Note:**

Some laptops or mobile devices may have separate wireless network switches, please make sure they are in the ON position.

3. Make sure the wireless network function of the router is enabled.
4. Check whether the WIFI driver is successfully installed in the device manager.

Q 4: IP address conflict occurs in the computer connecting to the router after starting up, how to solve this problem?

1. Please check whether there are other equipments that are using the identical IP address of the router assigned by DHCP server in the LAN. If there's any, please change the default gateway of the devices or the router to different network segment.
2. Check whether the LAN has other DHCP servers. If any, please close them.
3. Check LAN computers and whether there are computers using static IP address.

Q 5: What should I do if I forget the wireless encryption key of the wireless router?

1. Restore the router to factory default and then connect wireless network with encryption key on the back of the router.
2. Connect the wireless router and computer through cables. Log on the router setup page to check wireless encryption key in wireless security settings.

Q 6: Why I can use QQ, but cannot browse WebPages?

If QQ can be logged on, it means network connection is normal.

1. Make sure that the browser is normal or just change another browser to browse.
2. Check whether the network connection is configured with the correct DNS server address
3. Make sure the browser is set to never dial a connection and no proxy server is set.

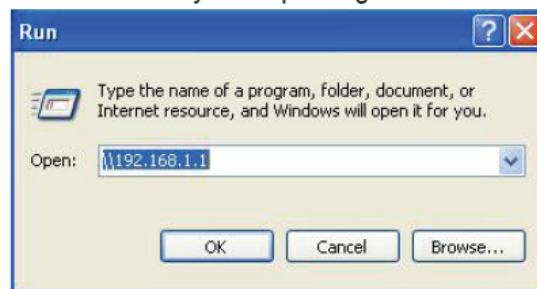
Q 7: What will affect wireless network signal?

1. Noise and interference. WLAN uses microwave transmission. Therefore, the microwave oven, radio telephone, Bluetooth device as well as same or adjacent wireless AP or router channel etc. will seriously affect transmission speed.
2. Structure of building. Wireless signal reaches wireless devices after multiple reflections in building, which results in transmission in several routes and interference with each other. Besides, greater energy loss will occur when wireless signal go through walls.
3. The location of the wireless router. The wireless router should be placed in a higher place to avoid blocking by other objects.
4. The antenna type of the wireless router. The antenna can be changed to strengthen signal.
5. External factors. Weather also greatly affects wireless signal. Cloudy and stormy weather can greatly weaken the signal.
6. Channel interference. It will cause great channel interference if there are multiple wireless routers on the same channel. Please try to switch to channels with less interference so that better wireless network environment could be obtained.

Q 8: How to access to shared files on USB devices?

1. Windows operating system.

1) The operations for checking shared files: enter “\\router LAN port IP address” in IE browser or press “Windows + R” keys to open Run Dialog Box; enter “\\router LAN port IP address” to access files shared by corresponding users.



2) Click “OK” and the following window appears. Enter the user name and password of the disk set up in the router and click “OK”. Shared files in the disk of the router could be

## **Appendix III Statement**

### **FCC Statement**

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference
- (2) This device must accept any interference received, including interference that may cause undesired operation.

This product has been tested and complies with the specifications for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which is found by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- (1) Reorient or relocate the receiving antenna
- (2) Increase the separation between the equipment or Devices
- (3) Connect the equipment to an outlet other than the receiver's
- (4) Consult a dealer or an experienced radio/TV technician for assistance

---

**FCC Caution:**

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

**FCC Radiation Exposure Statement**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your Body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter

**Safety Notices**

**WARNING:** Do not use this product near water, for example, in a wet basement or near a swimming pool.

**WARNING:** This product contains lead, known to the State of California to cause cancer, and birth defects or other reproductive harm. Wash hands after handling.

**WARNING:** Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightning.